Testimony of
William A. Reinsch
Under Secretary for Export Administration
Department of Commerce

Before
The Senate Commerce Committee
June 10, 1999

Thank you, Mr Chairman, for the opportunity to testify on the direction of the Administration's encryption policy. We have made a great deal of progress since my last testimony before this Committee on this subject.

Even so, encryption remains a hotly debated issue. The Administration continues to support a balanced approach which considers privacy and commerce as well as protecting important law enforcement and national security equities. We have been consulting closely with industry and its customers to develop a policy that provides that balance in a way that also reflects the evolving realities of the market place.

One of the many uses of the Internet which will have a significant affect on our everyday lives is electronic commerce. The Internet and other digital media are becoming increasingly important to the conduct of international business. There were 43.2 million Internet hosts worldwide last January compared to only 5.8 million in January 1995. According to a recent study, the value of e-commerce transactions in 1996 was $12 million. The projected value of e-commerce in 2000 is $2.16 billion. To cite one example, travel booked on Microsoft's Website has doubled every year since 1997, going from 500,000 to an estimated 2.2 million this year. Many service industries which traditionally required face-to-face interaction such as banks, financial institutions and retail merchants are now providing cyber service. Customers can now sit at their home computers and access their banking and investment accounts or buy a winter jacket with a few strokes of their keyboard.

Furthermore, most businesses maintain their records and other proprietary information digitally. They now conduct many of their day-to-day communications and business transactions via the Internet and E-mail. An inevitable byproduct of this growth of electronic commerce is the need for strong encryption to provide the necessary secure infrastructure for digital communications, transactions and networks. The disturbing increase in computer crime and electronic espionage has made people and businesses wary of posting their private and company proprietary information on electronic networks if they believe the infrastructure may not be secure. A robust secure infrastructure can help allay these fears, and allow electronic commerce to continue its explosive growth.

Developing an encryption policy has been complicated because we do not want to hinder its legitimate use -- particularly for electronic commerce; yet at the same time we want to protect our vital national security, foreign policy and law enforcement interests. We have concluded that the best way to accomplish this is to continue a balanced approach: to promote the development of strong encryption products that would allow lawful government access to plaintext under carefully defined circumstances; to promote the legitimate uses of strong encryption to protect confidentiality; and continue looking for additional ways to protect important law enforcement and national security interests.

During the past three years, we have learned that there are many ways to assist lawful access. There is no one-size-fits-all solution. The plans for recovery encryption products we received from more than 60 companies showed that a number of different technical approaches to recovery exist. In licensing exports of encryption products under individual licenses, we also learned that, while some products may not meet the strict technical criteria of our regulations, they are nevertheless consistent with our policy goals.

Additionally, we decided that the use of strong non-recovery encryption within certain trusted industry sectors is an important component of our policy to protect private consumer information and allow our U.S. high-tech industry to maintain its lead in the information security market. Taking into account all that we have learned and reviewing international market trends and realities, we made several changes in 1998 to our encryption policy that I will now summarize.

In September 1998, we published a regulation allowing the export, under a license exception, of unlimited strength encryption to banks and financial institutions located in 46 countries which allows U.S. companies new opportunities to sell encryption products to the world's leading economy. This policy recognizes the need to secure our financial networks, and the history of cooperation which the banking and financial communities have with government authorities when information is required to combat financial and other crimes.

More importantly, on September 16th, Vice President Gore unveiled an update to our encryption policy. This Policy Update was the result of a dialogue with U.S. industry, law enforcement, and privacy groups on how our policy might be improved to find technical solutions, in addition to key recovery, that can assist law enforcement in its efforts to combat crime. At the same time, we wanted to find ways to assure continued U.S. technology leadership, promote secure electronic commerce, and protect privacy concerns. We believed then and now that the best way to make progress on this issue is through a constructive, cooperative dialogue, rather than by legislative solutions. Through dialogue lasting more than a year, there has been increased understanding among the parties and we have made progress.

On December 31, we published regulations implementing the Vice President's policy announcement. These regulations will not end the debate over encryption controls, but we believe the regulation addresses some private sector concerns by opening large markets and further streamlining exports.

The Update permits the export of 128-bit encryption products and higher (with or without key recovery) to several important industry sectors. Now, banks, financial institutions, health facilities, and on-line merchants can secure their sensitive financial, medical, and on-line transactions in digital form. This update also allows U.S. companies to export 128-bit or greater encryption products, including technology to subsidiaries around the world, to protect its proprietary information and to develop new products. Further, this update allows the export of 128-bit or greater “recovery capable” or “recoverable” encryption products under an encryption licensing arrangement. Such products include those that are readily available in the marketplace such as general purpose routers, firewalls, and virtual private networks. These recoverable products are usually managed by a network or corporate security administrator without any involvement by a third party. Since the Update announcement, Industry has been taking advantage of this new liberalization and the streamlined process awarded to such products.

Many of the updates permit the export of encryption to these end-users under a license exception. That is, after the product receives a technical review, it can be exported by manufacturers, resellers and distributors without the need for a license or other additional review. These license exceptions currently apply to a list of countries or a set of end users. We also have a general policy of approval for exports to those sectors through encryption licensing arrangements (ELA), a kind of bulk license, to allow unlimited shipments of strong encryption to the sectors worldwide.

We also further streamlined exports of key recovery products by no longer requiring a review of foreign key recovery agents and no longer requiring companies to submit business plans.

We recognize that the development of our policy is an evolutionary process, and we intend to continue our dialogue with industry. Our policy will continue to adapt to technology and market changes. We will review our policy again this year with a view toward making further changes. An important component of our review is input from industry, which we are receiving through our continuing dialogue.

This past year, we also made progress on developing a common international approach to encryption controls through the Wassenaar Arrangement. Established in 1996 as the successor to COCOM, it is a multilateral export control arrangement among 33 countries whose purpose is to prevent destabilizing accumulations of arms and industrial equipment with military uses in countries or regions of concern. Wassenaar provides the basis for many of our export controls.

In December, through the hard work of Ambassador David Aaron, the President’s special envoy on encryption, the Wassenaar Arrangement members agreed on several changes relating to encryption controls. These changes go a long way toward increasing international security and public safety by providing countries with a stronger regulatory framework for managing the spread of robust encryption. Specific changes to multilateral encryption controls include removing multilateral controls on all encryption products at or below 56 bit and certain consumer items regardless of key length, such as entertainment TV systems, DVD products, and on cordless telephone systems designed for home or office use.

Most importantly, the Wassenaar members agreed to remove encryption software from Wassenaar’s General Software Note and replace it with a new cryptography note. Drafted in 1991, when banks, government and militaries were the primary users of encryption, the General Software Note allowed countries to export mass market encryption software without restriction. The GSN was created to release general purpose software used on personal computers, but it inadvertently also permitted countries to release encryption. It was essential to modernize the

GSN and close the loophole that permitted the uncontrolled export of encryption with unlimited key length. Under the new cryptography note, mass market hardware has been added and a 64-bit key length or below has been set as an appropriate threshold. This will lead governments to review the dissemination of 64-bit and above encryption.

I want to be clear that this does not mean encryption products of more than 64 bits cannot be exported. Our own policy permits that, as does the policy of most other Wassenaar members. It does mean, however, that such exports now can be reviewed by governments consistent with their national export control procedures.

Export control policies without a multilateral approach have little chance of success. Agreement among the Wassenaar members on the treatment of mass market encryption products is a strong indication that other countries share our public safety and national security concerns. Contrary to what many people thought two years ago, we have found that most major encryption producing countries are interested in developing a common approach to encryption controls.

The PROTECT Act

With respect to S.789, the Administration opposes this legislation for a number of reasons. Overall the bill does not promote the balance that this Administration has worked so hard to achieve over the past several years. Let me now discuss some of the more problematic sections.

Under section 505, the removal of export controls on publicly or generally available encryption is in effect left to an advisory board composed of private sector and government representatives, with the concurrence of the Secretary. We believe such a board would be unworkable. Although availability is one of the factors we use to decide whether an encryption product may be exported, it is not the only factor and should not be elevated above the others. We need to be able to take all factors, including national security and public safety, into account when making export control decisions. Disallowing or downgrading important considerations will only serve to weaken our export control system. The broad definitions used in the bill would give the Board wide latitude in making its findings on what is available. This could place the Secretary in the position of having to routinely object to the removal of export controls when important national security and law enforcement interests are at stake. The bill makes this decision subject to judicial review. The Administration does not think it is wise public policy for the courts to adjudicate Executive Branch decisions on these matters.

Section 501 removes the Department of Justice from the encryption export license consultation process. Since law enforcement interests are an important consideration in regard to encryption, we cannot support this provision.

We support the provisions in the bill that require a technical review for eligibility to export encryption under a license exception. In fact, this is consistent with current regulations. What we cannot support, however, is the portion of section 504 that would provide automatic eligibility after 15 days if the exporter has not received a decision from the government. In all cases, a very careful technical review is completed in order to determine that a product is technically eligible for a particular license exception. Although we try to perform these reviews as quickly as possible, a 15-day automatic approval will severely limit our ability to do a careful review.

Section 504 also proposes control parameters and export liberalizations beyond what the Administration can entertain and which would be contrary to our international export control obligations. For example, Wassenaar agreed to decontrol encryption products up to 56-bits whereas this bill would decontrol encryption products using a key length at 64-bits or less. Section 504 also expands the set of products, end users, and countries eligible to receive encryption under a license exception beyond what we believe is prudent.

Another troubling part of this bill is section 102, which would permit a U.S. person located anywhere in the world to develop, manufacture, sell or use any type of encryption. If this provision were construed to permit U.S. citizens to develop, manufacture and sell encryption products overseas, even with the use of non-public controlled technology that they had acquired in the United States, it would, in effect, prevent the government from requiring a license for U.S. persons to develop and manufacture encryption abroad. As a result, U.S. companies would likely move all development and manufacture of encryption out of the United States in order to take advantage of this loophole. This is not in our country's economic or national security interest.

Section 103 contains a provision that would prohibit the U.S. Government from conditioning any approval on the fact that a product is recoverable. A fundamental feature of our encryption policy is that we provide incentives for companies to develop products that provide strong security and also meet the needs of national security and law enforcement. The bill would eliminate this laudable feature of our policy that industry wanted us to include in last year's update. In addition, this provision of the bill is inconsistent with section 504 which allows license exception treatment for recoverable products.

Section 506 would eliminate any export controls on products using the forthcoming Advanced Encryption Standard (AES). We oppose the removal of export controls on encryption products simply because they implement a government standard. Products incorporating the AES should be exportable to the same extent as any other product incorporating encryption of similar strength. Under our current policy, AES-based products could be exported to banks, large corporations, on-line merchants without restriction and to many other safe endusers depending on the nature of the product. We do not think it is wise to link development of the AES to export controls. Such a linkage might bring undue pressure on NIST to complete the AES process faster than planned, and may therefore not allow prudent study of the security features of the candidate algorithms before selection.

With respect to the provisions of the bill that do not relate to export controls, we have a number of questions and concerns.

One such provision in Section 202 requires that encryption products used by the Government must interoperate with other commercial encryption products. The extent to which interoperability is required is unclear in the bill, but we believe the practical result of this requirement is that the Government could not use encryption because no single encryption product interoperates with all other products. It also appears that this provision could prohibit the use of encryption developed by the government for its own internal use in "closed" systems that are purposefully designed not to interoperate with other systems.

Section 202 also appears to prevent mandatory use of recoverable encryption when communicating with U.S. Federal, state and local governments. This would appear to preclude an agency from requiring key recovery or recoverable products for business purposes. We believe the effect of this provision may be much broader than simply preventing government from using recoverable encryption when dealing with the public. The practical effect would be that Government sites would have to be capable of supporting secure communications using all encryption methodologies on the market. This is absurd.

We are concerned that section 302 of the bill may preclude NIST's work with voluntary standards organizations because it prohibits the Secretary of Commerce from carrying out any policy that establishes an encryption standard for use by businesses or other entities other than for computer systems operated by the United States Government. The Secretary of Commerce is prohibited from establishing standards for business; however, when invited by standards organizations to do so, NIST does, as a matter of policy, work together with those organizations. Cooperation between NIST and standards organizations is important for both NIST and industry, and it is consistent with government policy to use voluntary standards and to purchase commercial off-the-shelf products. If the government cannot have input to the standards process, we may end up with less secure products available for government agencies. We want to encourage, to the extent possible, the development of voluntary standards that meet the needs of the government. This reduces costs for both government and industry.

In regard to section 401 dealing with the "Information Technology Laboratory," we have two concerns. First, we do not think it is appropriate for NIST to undertake research and development of new technologies to facilitate lawful access to communications and electronic information. This activity is more appropriately done by the FBI. Second, we are concerned that the bill will provide NIST with new tasks but no new funding to carry out this work. We have similar concerns with section 402. The advisory board, whose correct statutory name is " Computer System Security and Privacy Advisory Board," is made up of 13 volunteers. Again, any additional tasks assigned to this board would require necessary funding.

The Administration does not seek encryption export control legislation, nor do we believe such legislation is needed. The current regulatory structure provides for balanced oversight of export controls and the flexibility needed to adjust to our economic, foreign policy and national security interests to advances in technology. This is the best approach to an encryption policy that promotes secure electronic commerce, maintains U.S. lead in information technology, protects privacy, and protects public safety and national security interests.

As you know, public debate over encryption policy has been lively and often acrimonious. Some of those on both sides of the debate are not interested in searching for a middle ground that can meet all of our needs. Our dialogue with industry has gone a long way toward bridging that gap and finding common ground. We will continue this policy of cooperative exchange, which is clearly the best way to pursue our policy objectives of balancing public safety, national security, and the competitive interests of U.S. companies.